Fortschrittliche Sicherheit

← Zurück zu den Quicklinks

Mit den in Windows 10 integrierten Funktionen schützen Unternehmen ihre Benutzeridentitäten, Geräte, Apps, Daten und die IT-Infrastruktur. Darüber hinaus gibt Windows ihnen eine Reihe fortschrittlicher Hilfsmittel in die Hand, um ausgeklügelte Cyber-Attacken abzuwehren.

Device Guard

← Zurück zu den Quicklinks

- Malware eliminieren.

  Device Guard[1] setzt auf virtualisierungsbasierte Sicherheitstechnologien, um den Kernel zu isolieren und zu schützen. Der Device Guard Hyper-V Code Integrity Service (HVCI) schützt Prozesse, die im Kernelmodus laufen, vor speicherbasierten Angriffen, was insbesondere Zero-Day-Attacken und das Ausnutzen von Sicherheitslücken erschwert.

- Hardwarebasierte App-Kontrolle.

  Device Guard[1] schützt das Betriebssystem, indem der Codeintegritätsdienst parallel zum Kernel in einem per Windows-Hypervisor geschützten Container ausgeführt wird. Mithilfe von Signaturen, die Sie selbst über Richtlinien definieren können, legen Sie fest, was als vertrauenswürdig angesehen werden soll.

- Only run trusted apps.

  Mit Device Guard[1] kann die IT entscheiden, welche Softwareanbieter und Apps in Ihrer Netzwerkumgebung als vertrauenswürdig angesehen werden. Die IT kann dann diejenigen Apps und Anwendungen, die im Unternehmen bedenkenlos eingesetzt werden dürfen, festlegen. Dabei kann es sich um interne Geschäftsanwendungen, beliebige Apps aus dem Windows Store und Produkte einzelner Softwareanbieter handeln, da Device Guard sowohl Desktop-Anwendungen als auch Windows-Apps unterstützt.

Device Guard

- Kurztext

  Mithilfe von Device Guard[1] schützen Sie den Kernel von Windows 10 und verhindern, dass Malware, nicht autorisierte Apps und ausführbare Dateien auf den Geräten Ihres Unternehmens Schaden anrichten können.

- Mittellanger Text

  Mithilfe von Device Guard[1] schützen Sie den Kernel von Windows 10 vor digitalen Angriffen und verhindern, dass Malware, nicht autorisierte Apps und Anwendungen sowie ausführbare Dateien auf den Geräten Ihres Unternehmens Schaden anrichten können. Und indem Sie ausschließlich die Installation von Apps und Anwendungen aus vertrauenswürdigen Quellen zulassen, ist sichergestellt, dass Cyber-Angreifer keine Chance haben.

- Langtext

  Device Guard[1] setzt auf virtualisierungsbasierte Sicherheitstechnologien, um den Kernel zu isolieren und vor digitalen Angriffen zu schützen. Der Device Guard Hyper-V Code Integrity Service (HVCI) schützt Treiber und Prozesse, die im Kernelmodus laufen, vor speicherbasierten Angriffen, was insbesondere Zero-Day-Attacken und das Ausnutzen von Sicherheitslücken erschwert. Device Guard verhindert, dass Malware, nicht autorisierte Apps und Anwendungen sowie ausführbare Dateien auf den Geräten Ihres Unternehmens Schaden anrichten können. Und indem Sie ausschließlich die Installation von Apps und Anwendungen aus vertrauenswürdigen Quellen zulassen, ist sichergestellt, dass Cyber-Angreifer keine Chance haben.

- O-Ton

  „Device Guard[1], der bisher fortschrittlichste, in Windows integrierte Malware-Schutz, sorgt dafür, dass auf Ihren Geräten nur vertrauenswürdige Apps und Anwendungen verwendet werden können."

[1] Setzt Windows 10 Enterprise oder Windows 10 Education voraus.

Windows Defender Antivirus

← Zurück zu den Quicklinks

- Schützt Ihre Geräte von der ersten Sekunde an.

  Windows Defender Antivirus ist ein zuverlässiges Sicherheits-Tool, das einerseits von der Cloud profitiert und andererseits auf die Kombination aus künstlicher Intelligenz und Verhaltensanalyse setzt, um Ihre Geräte vor Viren und anderen digitalen Schädlingen zu schützen. Und mithilfe der Windows-Defender-Option „Cloudbasierter Schutz" lassen sich auch neue, weiterentwickelte und polymorphe Viren entdecken, sodass aus dem Internet geladene Dateien schnell und effizient als sicher oder unsicher eingestuft werden können.

- Erkennt Ransomware und verhindert, dass sie auf Ihren Geräten ausgeführt werden kann.

  Hat Ransomware ein Gerät befallen, setzt Windows Defender Antivirus eine Kombination aus verschiedenen datei- und verhaltensbasierten sowie kontextabhängigen Verfahren und Analysen ein, um zu verhindern, dass die Schadsoftware aktiviert werden kann. Schalten Sie die Windows-Defender-Option „Cloudbasierter Schutz" ein, steigert dies das Sicherheitslevel, da hierbei bei der Dateianalyse auch auf Informationen aus anderen Quellen zugegriffen wird, was die Erkennung von Ransomware-Attacken signifikant verbessert.

- Alle sicherheitsrelevanten Informationen auf einen Blick.

  Das mit Windows 10 Creators Update neu eingeführte Windows Defender Security Center ist die zentrale Anlaufstelle für alle Nutzer und informiert über den Viren- und Bedrohungsschutz, die Geräteleistung und –integrität sowie den Firewall- und Netzwerkschutz.

Windows Defender Antivirus

- Kurztext

  Windows Defender Antivirus ist in Windows 10 integriert. Das zuverlässige Sicherheits-Tool profitiert einerseits von der Cloud und setzt andererseits auf die Kombination aus künstlicher Intelligenz und Verhaltensanalyse, um Ihre Geräte vor Viren und anderen digitalen Schädlingen – darunter auch Ransomware – nachhaltig zu schützen.

- Mittellanger Text

  Das in Windows 10 integrierte Sicherheits-Tool Windows Defender Antivirus profitiert einerseits von der Cloud und setzt andererseits auf die Kombination aus künstlicher Intelligenz und Verhaltensanalyse, um Ihre Geräte vor Viren und anderen digitalen Schädlingen – darunter auch Ransomware – nachhaltig zu schützen. Mithilfe der Windows-Defender-Option „Cloudbasierter Schutz" lassen sich auch neue, weiterentwickelte und polymorphe Viren entdecken, sodass aus dem Internet geladene Dateien schnell und effizient als sicher oder unsicher eingestuft werden können.

- Langtext

  Das in Windows 10 integrierte Sicherheits-Tool Windows Defender Antivirus profitiert einerseits von der Cloud und setzt andererseits auf die Kombination aus künstlicher Intelligenz und Verhaltensanalyse, um Ihre Geräte vor Viren und anderen digitalen Schädlingen nachhaltig zu schützen. Mithilfe der Windows-Defender-Option „Cloudbasierter Schutz" lassen sich auch neue, weiterentwickelte und polymorphe Viren entdecken, sodass aus dem Internet heruntergeladene Dateien schnell und effizient als sicher oder unsicher eingestuft werden können. Hat Ransomware ein Gerät befallen, setzt Windows Defender Antivirus eine Kombination aus verschiedenen datei- und verhaltensbasierten sowie kontextabhängigen Verfahren und Analysen ein, um zu verhindern, dass die Schadsoftware aktiviert werden kann.

- O-Ton

  „Windows Defender Antivirus schützt Ihre Geräte zuverlässig vor aktuellen und zukünftigen digitalen Bedrohungen."

Windows Defender Advanced Threat Protection (ATP)

← Zurück zu den Quicklinks

• Unbekannte Bedrohungen entdecken.

ATP[1] erleichtert es Ihnen, ausgeklügelte Angriffe auf das Netzwerk sowie Datenlecks zu entdecken und die entsprechenden Maßnahmen zu ergreifen. Windows Defender ATP setzt bei der Erkennung auf die Kombination aus lokal ermittelten Daten, Informationen von Microsoft Intelligence Security Graph, künstlicher Intelligenz und Verhaltensanalyse. Diese Mischung ermöglicht es Windows Defender ATP, ausgeklügelte Angriffe auch dann zu erkennen, wenn sie lediglich Speicherbereiche betreffen oder kürzlich entdeckte Schwachstellen des Kernels ausnutzen.

• In Windows 10 integrierte, cloudbasierte Lösung.

ATP[1] vertraut auf ein Frühwarnsystem, das im Kernel des Betriebssystems integriert ist. Aus diesem Grund sind weder zusätzliche Komponenten, Clients und Signaturen, noch eine spezielle Vor-Ort-Infrastruktur erforderlich. Da die Sensoren des Frühwarnsystems Bestandteil von Windows 10 sind, lassen sie sich einfach aktivieren und verwalten. Windows Defender ATP wacht im Hintergrund und verbraucht nur geringe Systemressourcen, sodass weder die Netzwerkkapazität noch der Arbeitsspeicher über Gebühr belastet werden. Die Aktualisierung erfolgt über Windows as a Service. Sie können Windows Defender ATP problemlos zusammen mit einer Antiviruslösung eines Drittherstellers einsetzen, die Integration in Ihre bereits vorhandene Infrastruktur ist einfach.

• Die passenden Antworten auf Angriffe.

Entdeckt ATP[1] etwas Verdächtiges, wird die IT-Sicherheit alarmiert, damit sie die entsprechenden Gegenmaßnahmen einleiten kann. Diese Alarmmeldungen können – abgestuft nach der Schwere des Vorfalls – per E-Mail versandt werden. Sie können aber auch eigene Alarmmeldungen definieren, etwa um auf Gefahren, die in Ihrer IT-Umgebung eine große Rolle spielen, hingewiesen zu werden. Windows Defender ATP unterstützt Sie beim Sammeln zusätzlicher forensischer Daten und ermöglicht es der IT-Sicherheit, im Falle eines Angriffs die betroffenen Geräte zu isolieren und Dateien zu zerstören oder auf eine schwarze Liste zu setzen.

• Alle Informationen, die Sie benötigen.

ATP[1] bietet eine übersichtliche Protokollfunktion, die alle Informationen, die während der letzten sechs Monate erfasst wurden, abdeckt. Diese Informationen umfassen Geräte, Netzwerke, Dateien, Registry-Einträge, Nutzer, URLs und IP-Adressen. Darüber hinaus lassen sich auch die Ereignisse, die von Windows Defender Antivirus und Device Guard protokolliert wurden, einbinden. Dadurch kann auch lange Zeit nach einer Attacke die Vorgehensweise der Angreifer nachvollzogen werden. Windows Defender ATP nutzt Microsoft Intelligence Security Graph, um es Office 365 ATP-Abonnenten zu ermöglichen, auf verseuchten E-Mail-Anlagen basierende Angriffsversuche abzublocken und nachzuverfolgen.

[1] Zusätzliche Abonnements möglicherweise erforderlich.

Windows Defender Advanced Threat Protection (ATP)

• Kurztext

Windows Defender Advanced Threat Protection[1] (ATP) ermöglicht es Unternehmen, ausgeklügelte Angriffe und Zero-Day-Attacken auf das Netzwerk zu erkennen und die entsprechenden Gegenmaßnahmen zu ergreifen. Windows Defender ATP ist eine im Betriebssystem integrierte, cloudbasierte Lösung, die Microsoft Intelligence Security Graph unterstützt, sodass sie auch mit Office 365 ATP[1] zusammenarbeitet.

• Mittellanger Text

Windows Defender Advanced Threat Protection[1] (ATP) ermöglicht es Unternehmen, ausgeklügelte Angriffe und Zero-Day-Attacken auf das Netzwerk zu erkennen und die entsprechenden Gegenmaßnahmen zu ergreifen – ohne dazu eine spezielle Infrastruktur einrichten zu müssen. Windows Defender ATP greift auf Informationen aus verschiedenen Quellen zu und kombiniert sie mit künstlicher Intelligenz und Verhaltensanalyse, um Angriffe zu erkennen, die die anderen Schutzmechanismen überwunden haben. Die IT-Sicherheit, die bei Erkennung eines potenziellen Angriffs automatisch alarmiert wird, kann bei ihren Ermittlungen auf das Datenmaterial der letzten sechs Monate zurückgreifen.

• Langtext

Windows Defender Advanced Threat Protection[1] (ATP) ermöglicht es Unternehmen, ausgeklügelte Angriffe und Zero-Day-Attacken auf das Netzwerk zu erkennen und die entsprechenden Gegenmaßnahmen zu ergreifen. Eine spezielle Infrastruktur ist hierzu nicht erforderlich, da Windows Defender ATP direkt im Betriebssystem integriert ist. Windows Defender ATP greift auf lokale Daten und Informationen aus verschiedenen Quellen zu und kombiniert sie mit künstlicher Intelligenz und Verhaltensanalyse, um Angriffe zu erkennen, die die anderen Schutzmechanismen bereits überwunden haben. Die IT-Sicherheit, die bei Erkennung eines potenziellen Angriffs automatisch alarmiert wird, kann bei ihren Ermittlungen auf das Datenmaterial der letzten sechs Monate zurückgreifen. Diese Daten umfassen nicht nur Windows Defender ATP, sondern auch Windows Defender Antivirus und Device Guard. Windows Defender ATP nutzt Microsoft Intelligence Security Graph, um es Office 365 ATP[1] Abonnenten zu ermöglichen, auf verseuchten E-Mail-Anlagen basierende Angriffsversuche abzublocken und nachzuverfolgen.

• O-Ton

„Windows Defender Advanced Threat Protection[1] erleichtert es Unternehmen, ausgeklügelte Angriffe auf das Netzwerk sowie Datenlecks zu entdecken und die entsprechenden Maßnahmen zu ergreifen."

Credential Guard

← Zurück zu den Quicklinks

- Schützt Anmeldeinformationen auch dann, wenn der Kernel kompromittiert wurde.

  Credential Guard[1] ist einer von mehreren, in Windows 10 integrierten Mechanismen zum Schutz der Benutzerkonten. Die Funktion schützt die Benutzer-Zugriffstoken, die bei der Authentifizierung generiert werden. Der Schutz dieser Token ist zur Abwehr von NTLM Pass-the-Hash-Angriffen, die die am häufigsten genutzten Vorgehensweisen bei Attacken auf das Netzwerk darstellen, von entscheidender Bedeutung. Credential Guard speichert die Token in einer virtualisierungsbasierten Sicherheitsumgebung, die als eigene Instanz über die Hyper-V-Technologie ausgeführt wird. So wird verhindert, dass Angreifer die Token von Geräten extrahieren – und zwar auch dann, wenn der Windows-Kernel bereits kompromittiert wurde.

- Umfassende Sicherheit auf Hardwareebene.

  Credential Guard[1] setzt eine Kombination aus hardwarebasierter Virtualisierung und Hyper-V ein, um die Benutzer-Zugriffstoken zu isolieren und vor Angriffen zu schützen. Die Isolierung erfolgt dabei hardwarebasiert, sodass Malware und Angreifer nicht einmal dann auf die Anmeldeinformationen eines Nutzers zugreifen können, wenn sie sich die höchsten Privilegien angeeignet haben.

- Einfache Verwaltung.

  Credential Guard[1] kann über Gruppenrichtlinien aktiviert werden und lässt sich somit ganz einfach mit den bereits vorhandenen Verwaltungstools administrieren.

Credential Guard

- Kurztext

  Credential Guard[1] schützt Single-Sign-In-Benutzertoken (NTLM) vor Diebstahl und Missbrauch, indem diese Informationen in einem sicheren, hardwareisolierten Container gespeichert werden.

- Mittellanger Text

  Credential Guard[1] schützt Single-Sign-In-Benutzertoken vor Diebstahl und verhindert so, dass Angreifer, die mit einer falschen Identität versuchen, auf das Netzwerk zuzugreifen, Erfolg haben. Die sensiblen Informationen werden in einem sicheren, hardwareisolierten Container gespeichert, sodass sie nicht einmal dann in falsche Hände gelangen können, wenn das Gerät kompromittiert wurde.

- Langtext

  Die in Windows 10 integrierte Funktion Windows Hello[2] stellt eine komfortable und sichere Authentifizierungsmethode dar. Credential Guard[1] geht noch einen Schritt weiter, um zu verhindern, dass Angreifer unter Zuhilfenahme einer falschen Identität Zugriff auf das Netzwerk erhalten. Credential Guard schützt die Single-Sign-In-Benutzertoken, die generiert werden, sobald die Identität eines Benutzers bestätigt wurde, indem diese Elemente vom Windows-Kernel isoliert und in einer sicheren, virtualisierten Hyper-V-Umgebung gespeichert werden. Dadurch können diese Informationen nicht einmal dann in falsche Hände gelangen, wenn das Gerät kompromittiert wurde. Dieser Schutzmechanismus spielt unter anderem bei der Abwehr von NTLM Pass-the-Hash-Angriffen, die die am häufigsten genutzten Vorgehensweisen bei Attacken auf das Netzwerk darstellen, eine große Rolle.

- O-Ton

  „Credential Guard schützt die Benutzeranmeldeinformationen, indem es eine der häufigsten Vorgehensweisen zur Kompromittierung von Geräten und Netzwerken aushebelt."

[1] Setzt Windows 10 Enterprise oder Windows 10 Education voraus. Setzt UEFI 2.3.1 oder aktueller mit Trusted Boot voraus; Virtualisierungserweiterungen wie Intel VT-x, AMD-V und SLAT müssen aktiviert sein; nur für die x64-Bit-Editionen von Windows; IOMMU, etwa Intel VT-d und AMD-Vi; BIOS Lockdown; TPM 2.0 empfohlen für Zertifizierung der Geräteintegrität (steht TPM 2.0 nicht zur Verfügung, kommt Software zum Einsatz) [2] Windows Hello erfordert spezielle Hardware, darunter einen Fingerabdruckleser, einen aktiven IR-Sensor oder andere biometrische Sensoren.

Windows Hello

← Zurück zu den Quicklinks

• Schnell, sicher – und ohne Passwort.

Dank Windows Hello[1] melden Sie sich an Ihren Windows-Geräten, kompatiblen Apps und Webseiten dreimal schneller an[3] als mit einem Passwort. Denn während Sie sich ein Passwort merken, es eintippen und in regelmäßigen Abständen ändern müssen, authentifizieren Sie sich bei Windows Hello ganz einfach mit Ihrem Gesicht, Ihrem Fingerabdruck, einer PIN oder einem Windows Hello-Begleitgerät[4].

• Viel sicherer als ein Passwort.

Entsperren Sie Ihr Gerät mit Ihrem Gesicht oder Fingerabdruck, ist maximale Sicherheit gewährleistet. Windows Hello[1] setzt bei der Authentifizierung auf mindestens zwei Faktoren, etwa Biometrie und Ihr Gerät. Die Biometrie, etwa per Gesichtserkennung oder mittels Fingerabdruckscanner, stellt die mit Abstand komfortabelste Form der Authentifizierung dar und ist zudem um ein Vielfaches sicherer als ein Passwort. Und sie funktioniert auf allen Geräten, die mit Windows 10 ausgestattet sind.

• Anmeldeinformationen vor Diebstahl/Missbrauch geschützt.

Das in Ihrem Gerät verbaute Trusted Platform Module (TPM) isoliert Ihre Windows-Anmeldeinformationen vom Betriebssystem, sodass sie vor Malware und ausgeklügelten Angriffen geschützt sind. Windows Hello[1] basiert auf dem Sicherheitsstandard FIDO 2.0 und ist somit nicht nur resistent gegenüber Phishing-Angriffen, sondern bietet auch einen erweiterten Schutz vor Datenlecks in Rechenzentren, indem die Authentifizierungsinformationen getrennt von den Windows-Hello-Zugangsdaten gespeichert werden. Selbst wenn Sie Ihre PIN auf einer gefälschten Webseite eingeben, haben Angreifer keine Chance, da sie nicht im Besitz Ihres Geräts sind.

• Windows Hello nicht auf Windows-Anmeldung beschränkt.

Vergessen Sie Passwörter. Windows Hello[1] funktioniert mit Office 365[5] und anderen Microsoft-Diensten, Azure Apps[3] wie Dynamics CRM[6], und ist zudem kompatibel mit Dritthersteller-Apps und -Anwendungen wie Dropbox[6]. Aber auch auf Webseiten, die Windows Hello unterstützen, können Sie sich schnell und sicher einloggen – sofern Sie Microsoft Edge[2] nutzen.

Windows Hello

• Kurztext

Windows Hello[1] ist eine komfortable, auch für Unternehmen optimal geeignete Alternative zu Passwörtern. Die Authentifizierung basiert auf drei Faktoren: Biometrie, PIN-Eingabe und Begleitgerät[4].

• Mittellanger Text

Windows Hello[1] ist eine komfortable und aufgrund der hohen Sicherheit auch für Unternehmen optimal geeignete Alternative zu Passwörtern. Die Authentifizierung basiert auf drei Faktoren: Biometrie (Gesichts- oder Fingerabdruckerkennung), PIN-Eingabe und Begleitgerät[4]. Zusätzliche Hardware oder eine spezielle Infrastruktur sind nicht erforderlich. Und da Windows Hello auf dem Sicherheitsstandard FIDO 2.0 basiert, ist dieses Authentifizierungsverfahren nicht nur resistent gegenüber Phishing-Angriffen, sondern bietet auch einen erweiterten Schutz vor Datenlecks in Rechenzentren.

• Langtext

Windows Hello[1] ist eine komfortable und aufgrund der extrem hohen Sicherheit optimal geeignete Alternative zu Passwörtern und Smartcards - auch für Unternehmen, die in stark regulierten Branchen tätig sind sowie für Behörden. Die Authentifizierung basiert auf drei unterschiedlichen Faktoren: Biometrie (Gesichts- oder Fingerabdruckerkennung), PIN-Eingabe und Begleitgerät[4]. Zusätzliche Hardware oder eine spezielle Infrastruktur sind zur Nutzung nicht erforderlich. Und da Windows Hello auf dem Sicherheitsstandard FIDO 2.0 basiert, ist dieses Authentifizierungsverfahren nicht nur resistent gegenüber allen Arten von Phishing-Angriffen, sondern bietet auch einen erweiterten Schutz vor Datenlecks in Rechenzentren.

• O-Ton

„Windows Hello ist ein einfach bereitzustellendes, komfortables Multifaktor-Authentifizierungsverfahren, das maximale Sicherheit bei minimalem Aufwand bietet."

[1] Windows Hello erfordert spezielle Hardware, darunter einen Fingerabdruckleser, einen aktiven IR-Sensor oder andere biometrische Sensoren. Der hardwarebasierte Schutz der Windows-Hello-Anmeldedaten setzt TPM 1.2 oder aktueller voraus, steht TPM nicht zur Verfügung oder ist TPM nicht konfiguriert, kommt der softwarebasierte Schutz zum Einsatz. [2] Nur kompatible Webseiten und Apps/Anwendungen. [3] Basiert auf dem durchschnittlichen Zeitvergleich zwischen Eingabe eines Passwortes und der Erkennung eines Gesichts oder Fingerabdrucks bis zur erfolgreichen Authentifizierung. [4] Begleitgerät muss mittels Bluetooth mit dem Windows 10-Gerät gekoppelt sein. Um ein Windows-Hello-Begleitgerät zur Anmeldung an einem anderen Windows 10-Gerät zu verwenden, muss auf dem mit dem Begleitgerät gekoppelten System Windows 10 Pro oder Windows 10 Enterprise laufen. [5] Separat erhältlich. [6] Verfügbar für ausgewählte Premium-Smartphones und ausgewählte Windows 10-Editionen. Sowohl PC als auch Smartphone müssen bei Azure Active Directory oder Active Directory angemeldet und mittels Bluetooth gekoppelt sein.

Windows Information Protection

← Zurück zu den Quicklinks

- Strikte Trennung zwischen privaten und unternehmenseigenen Daten.

  Windows Information Protection[1] (WIP) erhöht in Unternehmen die Sicherheit, indem die Funktion zwischen privaten und geschäftlichen Daten trennt und so eine versehentliche Weitergabe oder Veröffentlichung sensibler Informationen verhindert. Die IT kann eigene Regeln definieren, um festzulegen, wie unternehmenseigene Daten verwendet werden dürfen. WIP erkennt anhand der Software, mit der die Daten erstellt wurden, dass es sich um unternehmenseigene Informationen handelt. Darüber hinaus kann diese Klassifizierung auch durch den Nutzer erfolgen.

- Strenge Kontrolle von Benutzer- und App-Zugriffen.

  Windows Information Protection[1] (WIP) gestattet es der IT, Richtlinien zu definieren, in denen festgelegt ist, welche Applikationen und Nutzer auf unternehmenseigene Daten zugreifen dürfen. Dadurch kann verhindert werden, dass sensible Informationen versehentlich oder absichtlich auf Webseiten eingegeben oder in persönliche Dokumente eingefügt werden. Dieser Schutz umfasst aber auch Daten, die auf portablen Speichermedien abgelegt werden. In solchen Fällen werden alle Daten verschlüsselt, sodass ausschließlich autorisierte Nutzer darauf zugreifen können.

- Die IT hat die volle Kontrolle über die unternehmenseigenen Daten.

  Die in Windows 10 Pro und Windows 10 Enterprise integrierte Funktion Windows Information Protection[1] (WIP) kümmert sich im Hintergrund um den Schutz der unternehmenseigenen Daten. Der Nutzer merkt davon nichts. Lediglich wenn versucht wird, mit WIP geschützte Daten weiterzugeben, wird ein Warnhinweis ausgegeben, der den Nutzer darauf aufmerksam macht. Die IT hat die volle Kontrolle über die Schlüssel und geschützte Daten und ist in der Lage, die auf einem Privatgerät gespeicherten Unternehmensdaten bei Bedarf aus der Ferne zu löschen[2]. Alle persönlichen Inhalte bleiben dabei erhalten.

Windows Information Protection

- Kurztext

  Windows Information Protection[1] (WIP) beugt der versehentlichen als auch gewollten Weitergabe unternehmenseigener Daten vor, indem der Benutzer- und App-Zugriff basierend auf Richtlinien, die vom Unternehmen festgelegt werden, geregelt wird.

- Mittellanger Text

  Windows Information Protection[1] (WIP) bietet Ihnen Sicherheit auf Unternehmensniveau – bei einfacher Verwaltung und Nutzung. Im Gegensatz zu einem Großteil der Drittherstellerlösungen verzichtet WIP auf Container, spezielle Apps und besondere Betriebsmodi. Vielmehr fungiert WIP als eine Art Wächter, der Nutzern und Apps ausschließlich Zugriff auf diejenigen Informationen gestattet, die Sie mithilfe von Richtlinien festgelegt haben. Da WIP in die mobilen und Desktop-Plattformen integriert ist, profitieren Sie auf all Ihren Windows-Geräten davon.

- Langtext

  Die in Windows 10 integrierte Funktion Windows Information Protection[1] (WIP) beugt der versehentlichen als auch gewollten Weitergabe unternehmenseigener Daten vor – bei einfacher Verwaltung und Nutzung. Im Gegensatz zu einem Großteil der Drittherstellerlösungen verzichtet WIP auf Container, spezielle Apps und besondere Betriebsmodi. Vielmehr fungiert WIP als eine Art Wächter, der Nutzern und Apps ausschließlich Zugriff auf diejenigen Informationen gestattet, die Sie mithilfe von Richtlinien festgelegt haben. Die IT hat die volle Kontrolle über die Schlüssel und geschützte Daten und ist in der Lage, die auf einem Privatgerät gespeicherten Unternehmensdaten bei Bedarf aus der Ferne zu löschen[2]. WIP ist in die mobilen und Desktop-Plattformen integriert, sodass Sie auf all Ihren Windows-Geräten davon profitieren, ohne zusätzliche Software installieren zu müssen. WIP unterstützt Azure Information Protection und Office 365, sodass sich Unternehmensdaten auch in komplexeren Infrastrukturen nachhaltig schützen lassen.

- O-Ton

  „Windows Information Protection[1] (WIP) beugt der versehentlichen als auch gewollten Weitergabe unternehmenseigener Daten vor, und ist einfach bereitzustellen, zu bedienen und zu verwalten."

[1] Zur Verwaltung der Einstellungen von WIP sind entweder Mobile Device Management (MDM) oder System Center Configuration Manager erforderlich. Diese Produkte sind separat erhältlich. Active Directory erleichtert die Verwaltung, ist aber nicht zwingend erforderlich. [2] Zur Fernlöschung ist ein Verwaltungssystem (separat erhältlich) erforderlich.

Windows Trusted Boot

← Zurück zu den Quicklinks

- Volle Kontrolle – schon beim Hochfahren.

  Die in Windows 10 integrierte Funktion Windows Trusted Boot stellt sicher, dass während des Startvorgangs ausschließlich vertrauenswürdige Software und Komponenten geladen werden. Fährt der PC hoch, wird überprüft, ob die Gerätefirmware, alle im Zusammenhang mit dem Bootvorgang stehenden Komponenten sowie die verwendete Antiviruslösung vertrauenswürdig sind. Auf diese Weise soll verhindert werden, dass Malware vor oder während des Hochfahrens aktiviert werden kann.

- Gefahr erkannt, Gefahr gebannt.

  Windows Trusted Boot sorgt dafür, dass der Windows-Systemkern erst dann geladen werden kann, wenn seine Integrität bestätigt wurde. Dies schützt Ihre Geräte vor ausgeklügelten Angriffen. Werden Anomalien entdeckt, beseitigt Windows Trusted Boot das Problem in Eigenregie, sodass das sichere Hochfahren gewährleistet ist.

- Vertrauen ist gut, Kontrolle ist besser.

  Mit Windows Trusted Boot lässt sich die Integrität eines Geräts schnell und einfach verifizieren. Wer mehr Kontrolle benötigt, profitiert davon, dass Windows Trusted Boot auf die cloudbasierte Dienstverwaltung Device Health Attestation (DHA) zurückgreift. Denn dadurch können Sie mit Verwaltungssystemen wie Microsoft Intune[1] und System Center Configuration Manager[1] die Integrität eines Geräts bestätigen, bevor es auf Netzwerkressourcen zugreifen darf.

Windows Trusted Boot

- Kurztext

  Windows Trusted Boot sichert den Start Ihrer Windows 10-PCs ab, indem ausschließlich vertrauenswürdige Komponenten geladen werden. Auf diese Weise ist sichergestellt, dass Malware, die sich bereits im System eingenistet hat, keinesfalls vor dem Betriebssystem aktiv werden kann.

- Mittellanger Text

  Windows 10 verhindert, dass Malware beim PC-Start vor dem Betriebssystem geladen werden kann. Windows Trusted Boot stellt im Zusammenspiel mit UEFI Secure Boot sicher, dass beim Hochfahren ausschließlich vertrauenswürdige Komponenten und Software ausgeführt werden. Dazu wird die Integrität aller Betriebssystemkomponenten, Treiber und kompatiblen Anti-Malware-Lösung überprüft.

- Langtext

  Windows Trusted Boot sichert den Start Ihrer Windows 10-PCs ab, indem ausschließlich vertrauenswürdige Komponenten geladen werden. Auf diese Weise ist sichergestellt, dass Malware, die sich bereits im System eingenistet hat, keinesfalls vor dem Betriebssystem aktiv werden kann.

  Windows Trusted Boot kann zusammen UEFI Secure Boot, einem Hardwarestandard, der von den führenden IT-Unternehmen entwickelt wurde, eingesetzt werden. Sobald der PC startet, überprüft die UEFI-Firmware die Signaturen aller Betriebssystem- und Softwarekomponenten, die während des Bootens geladen werden, um zu verhindern, dass Malware vor dem Betriebssystem aktiviert werden kann. Anschließend stellt Windows Trusted Boot sicher, dass die Integrität aller Betriebssystemkomponenten, Treiber und kompatiblen Anti-Malware-Lösung gewährleistet ist.

- O-Ton

  „Windows Trusted Boot erleichtert es Ihnen, die Integrität der Gerätefirmware und des Betriebssystems bereits beim Start Ihrer Windows 10-PCs zu überprüfen, um sicherzustellen, dass die Geräte nicht mit Malware versucht sind. Dadurch verhindern Sie, dass kompromittierte Geräte auf Unternehmensressourcen zugreifen und steigern den Schutz vor aktuellen Sicherheitsbedrohungen."

[1] Separat erhältlich.

BitLocker

← Zurück zu den Quicklinks

- Sicherheit bei Verlust des Geräts

  Selbst wenn ein Gerät verloren geht oder gestohlen wird, ist sichergestellt, dass die darauf gespeicherten Daten nicht in die Hände Unbefugter gelangen können.

  Mit BitLocker und BitLocker To Go verschlüsseln Sie Ihre Daten auf Festplatten und portablen USB-Speichermedien[1].

BitLocker

- Kurztext

  Mit BitLocker[1] können Unternehmen sensible Daten diebstahlsicher verschlüsseln, sodass sie nicht einmal dann in die Hände Dritter gelangen können, wenn ein Gerät verloren geht oder gestohlen wird. Dies vereinfacht es Unternehmen, regulatorische Vorgaben und Compliance-Richtlinien einzuhalten.

- Mittellanger Text

  Mit BitLocker[1] können Unternehmen sensible Daten diebstahlsicher verschlüsseln, sodass sie nicht einmal dann in die Hände Dritter gelangen können, wenn ein Gerät verloren geht oder gestohlen wird. Dies vereinfacht es Unternehmen, regulatorische Vorgaben und Compliance-Richtlinien einzuhalten. Die IT verschlüsselt mit BitLocker einzelne Partitionen oder komplette Laufwerke, für den Schutz von USB-Speichermedien verwenden Sie BitLocker To Go.

- Langtext

  Mit BitLocker[1] können Unternehmen sensible Daten diebstahlsicher verschlüsseln, sodass sie nicht einmal dann in die Hände Dritter gelangen können, wenn ein Gerät verloren geht oder gestohlen wird. Dies vereinfacht es Unternehmen, regulatorische Vorgaben und Compliance-Richtlinien einzuhalten. Die IT verschlüsselt mit BitLocker einzelne Partitionen oder komplette Laufwerke, für den Schutz von USB-Speichermedien verwenden Sie BitLocker To Go. Microsoft BitLocker Administration and Monitoring (MBAM) gibt der IT alle Werkzeuge in die Hand, die erforderlich sind, um mit BitLocker verschlüsselte Umgebungen bereitzustellen und zu verwalten. Darüber hinaus erleichtert MBAM die Provisionierung, die Überwachung und Protokollierung der Compliance-Einstellungen und – im Falle eines Hardwaredefekts – die Wiederherstellung der verschlüsselten Daten.

- O-Ton

  „BitLocker[1] erleichtert es Unternehmen, regulatorische Vorgaben und Compliance-Richtlinien einzuhalten, indem sensible Daten diebstahlsicher verschlüsselt werden, sodass sie nicht einmal dann in die Hände Unbefugter gelangen können, wenn Geräte verloren gehen oder gestohlen werden."

[1] Für TPM-basierten Schlüsselschutz ist TPM 1.2 oder höher erforderlich.